Cybersecurity Incident Report: Distributed Denial of Service (DDoS) Attack

Identify

The organization experienced a DDoS attack that overwhelmed the internal network for approximately two hours. The attack consisted of a flood of ICMP packets entering the network through an unconfigured firewall. The systems most impacted were the company's internal network services, which stopped responding to legitimate traffic. The cause was traced to the lack of proper firewall configuration, which allowed attackers to exploit ICMP traffic to launch the attack.

Protect

The company needs to strengthen its firewall configurations and network security policies. Specific improvements include enforcing firewall rules that limit ICMP traffic, applying access control measures to prevent spoofed IP addresses, and providing staff training on network hardening practices. In addition, non-critical services should have predefined procedures to be taken offline quickly during attacks, ensuring that critical services remain prioritized.

Detect

Improved monitoring is required to catch abnormal network traffic early. The organization has begun using network monitoring software and IDS/IPS systems to flag suspicious ICMP traffic patterns. Continuous log analysis, traffic baselining, and automated alerts will help detect similar attacks faster in the future. Regular audits of firewall configurations and device logs should also be performed to ensure no gaps remain.

Respond

The incident response involved blocking incoming ICMP packets, shutting down non-critical services, and restoring critical ones. Going forward, the response plan should include automated rate limiting of ICMP traffic, playbooks for rapid service isolation, and pre-approved escalation steps for the incident response team. Analysis of traffic logs should be used after each incident to fine-tune detection and prevention controls.

Recover

Recovery focused on restoring normal operations for affected network services. Critical processes were restored first, followed by non-critical ones once stability was confirmed. To improve future recovery, the organization should implement backup communication channels for business continuity, maintain recovery runbooks, and schedule periodic recovery drills. This will ensure the organization can recover quickly and maintain stakeholder trust after any disruption.